PATENT ABSTRACTS OF JAPAN

JPA08-137733

(11)Publication number : 08-137733
(43)Date of publication of application : 31.05.1996

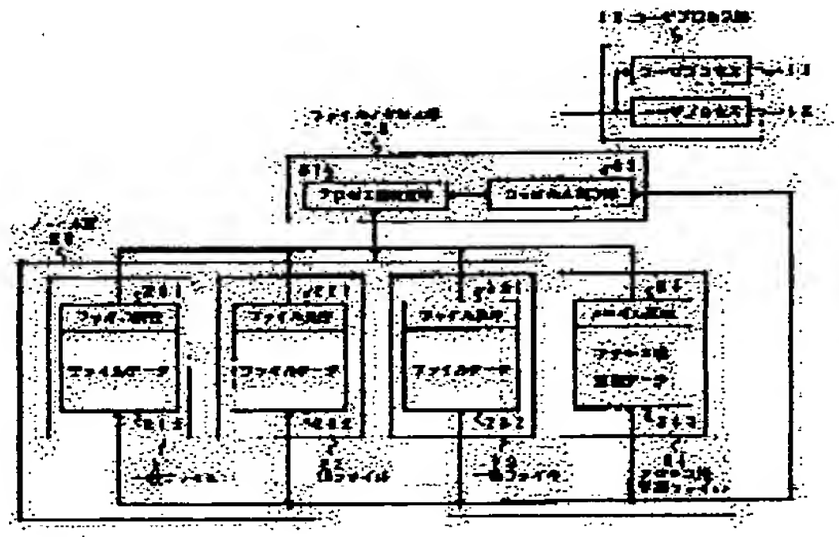
(51)Int.Cl. G06F 12/00

(21)Application number : 06-272059
(22)Date of filing : 07.11.1994

(71)Applicant : NEC CORP
(72)Inventor : SHIMIZU YASUHIRO

(54) SECURITY PROTECTION SYSTEM

(57)Abstract:
PURPOSE: To protect the security of a file in the operating system of a multiuser.
CONSTITUTION: Access right levels showing the access priority of the file are included in file attributes (211, 221, 231 and 241). An access right definition file (24) where the access right level is defined when the user accesses all the files is set. The user concerned judges whether access is possible or not by comparing two kinds of access right levels. Thus, it is not necessary to define a data format at every application program, and the compatibility of a data file and the program can be held.



LEGAL STATUS

[Date of request for examination] 07.11.1994
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2713186
[Date of registration] 31.10.1997
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right] 31.10.2001

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平8－137733

(43)公開日　平成8年(1996)5月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI	技術表示箇所
G06F 12/00	537 A	7623－5B		

審査請求　有　　請求項の数3　OL　（全 5 頁）

(21)出願番号　特願平6－272059

(22)出願日　平成6年(1994)11月7日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72)発明者　清水　靖浩
東京都港区芝五丁目7番1号　日本電気株式会社内

(74)代理人　弁理士　後藤　洋介　（外2名）

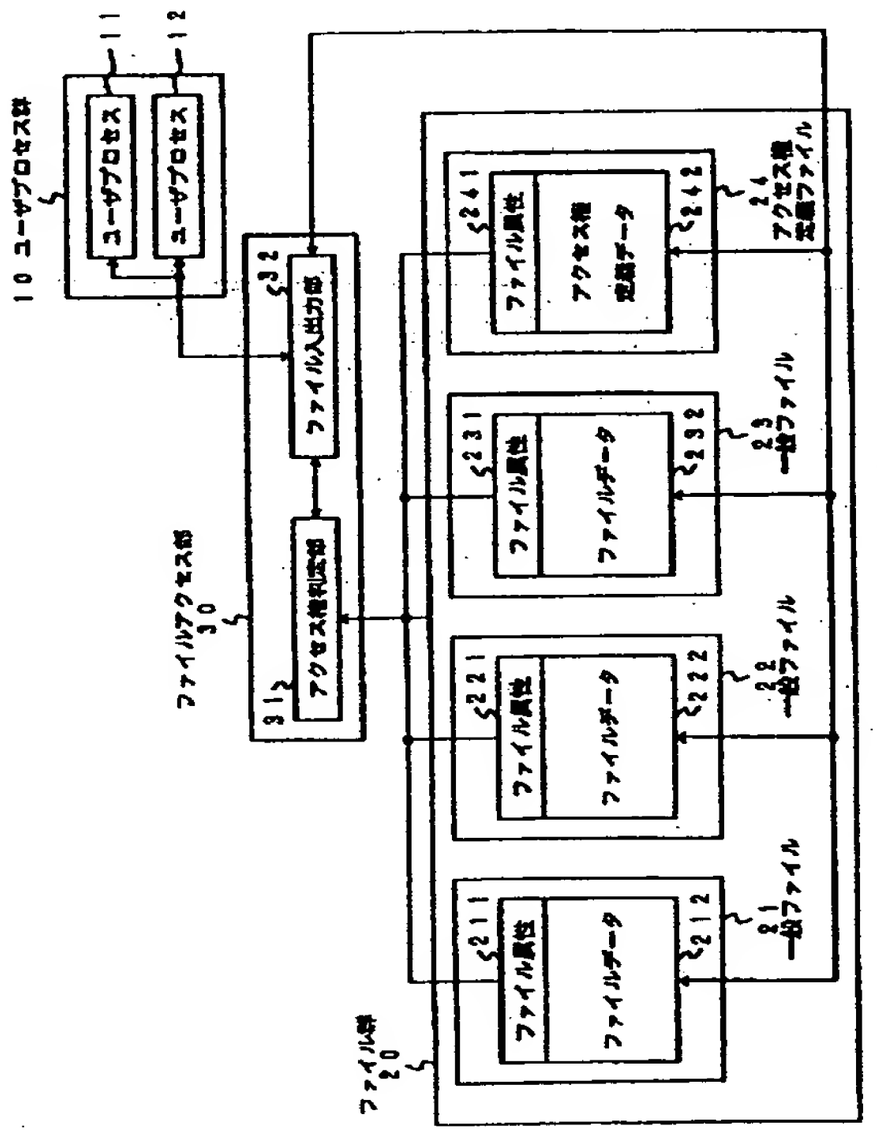
(54)【発明の名称】　機密保護方式

(57)【要約】

【目的】　マルチユーザのオペレーティングシステムにおけるファイルの機密保護を図る。

【構成】　ファイルのアクセス優先度を示すアクセス権レベルをファイル属性（２１１，２２１，２３１，２４１）に含ませ、ユーザーが全ファイルをアクセスする場合のアクセス権レベルを定義したアクセス権定義ファイル（２４）を設定する。前記２種類のアクセス権レベルを比較することにより、当該ユーザがアクセス可能か否かを判断する。

【効果】　アプリケーションプログラムごとにデータフォーマットを定義する必要がなくなり、データファイルやプログラムの互換性を保つことができる。



【特許請求の範囲】

【請求項１】　複数のユーザプロセスがファイル群をアクセス可能な計算機システムにおいて、前記ファイル群は、複数のファイルとアクセス権定義ファイルとから成り、前記複数のファイルにはそれぞれ、ファイルに対するアクセスの優先度を示すアクセス権レベルがファイル属性として含まれ、前記アクセス権定義ファイルには各ユーザプロセスの全ファイルに対するアクセスの優先度を示すアクセス権レベルが予め定義されており、前記ファイル群と前記複数のユーザプロセスとの間にはファイルアクセス部を有し、該ファイルアクセス部は、ユーザプロセスがファイルをアクセスするとき、ファイル属性を読み込み、この属性の中のアクセス権レベルと前記アクセス権定義ファイル中の当該ユーザプロセスの全ファイルに対するアクセス権レベルとを比較して、前者のアクセス権レベルが高ければアクセス要求を拒否し、後者のアクセス権レベルの方が高ければアクセス要求を許可することを特徴とする機密保護方式。

【請求項２】　請求項１記載の機密保護方式において、前記アクセス権定義ファイルは、前記複数のファイルに対するアクセス権レベルである読出しレベル，書込レベル，実行レベルを予め定義したアクセス権定義データを格納していることを特徴とする機密保護方式。

【請求項３】　請求項２記載の機密保護方式において、前記ファイルアクセス部は、アクセス権判定部とファイル入出力部とを有し、前記ファイル入出力部は、ユーザプロセスからファイルのアクセス要求があると、前記ファイル群から要求ファイルの属性の情報を取得して、前記アクセス権判定部を呼び出し、前記アクセス権判定部は、呼び出しがあるとファイル属性の情報を読み出し、ユーザプロセスがファイルの所有者である場合には、所有者の属性に従ってアクセス判定を行い、ユーザが所有者でない場合にはファイル属性で定義しているその他ユーザのアクセス権レベルと前記アクセス権定義データ中のアクセス権レベルとを比較して、前者のアクセス権レベルが高ければアクセス要求を拒否し、後者のアクセス権レベルの方が高ければアクセス要求を許可することを特徴とする機密保護方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は機密保護方式に関し、特にマルチユーザのオペレーティングシステムのファイル保護方式に関する。

【０００２】

【従来の技術】従来、プロセスがファイルをアクセスする場合のファイル保護は次のようにして行われている。まず、ファイルの割当またはオープン処理で要求プロセスがこのファイルをアクセスする権利があるかないかをオペレーティングシステムがファイル属性により判断するようにしている。そして、アクセス権があるときは当該プロセスが当該ファイル内よりレコードを読み込み、その一部に含まれるレコードのアクセスの可否情報やレコードのアクセスレベルとプロセスのアクセスレベルとの比較をし、アクセス権がある場合にはファイル中の当該レコードのみをアクセスできる。このような保護方式は、例えば特開平１－７１４６、特開昭６２－２６０２３８に示されている。

【０００３】

【発明が解決しようとする課題】上記のように、従来の保護方式は、ファイル中のデータの一部にアクセスレベルを定義してアプリケーションプログラムで管理する方式であったため、各アプリケーションプログラムごとにデータフォーマットを定義する必要があり、データやプログラムの互換性を損なうという欠点があった。また、アプリケーションプログラムから実行形式のファイルに対する機密保護をすることができないという欠点があった。

【０００４】

【課題を解決するための手段】本発明によれば、複数のユーザプロセスがファイル群をアクセス可能な計算機システムにおいて、前記ファイル群は、複数のファイルとアクセス権定義ファイルとから成り、前記複数のファイルにはそれぞれ、ファイルに対するアクセスの優先度を示すアクセス権レベルがファイル属性として含まれ、前記アクセス権定義ファイルには各ユーザプロセスの全ファイルに対するアクセスの優先度を示すアクセス権レベルが予め定義されており、前記ファイル群と前記複数のユーザプロセスとの間にはファイルアクセス部を有し、該ファイルアクセス部は、ユーザプロセスがファイルをアクセスするとき、ファイル属性を読み込み、この属性の中のアクセス権レベルと前記アクセス権定義ファイル中の当該ユーザプロセスの全ファイルに対するアクセス権レベルとを比較して、前者のアクセス権レベルが高ければアクセス要求を拒否し、後者のアクセス権レベルの方が高ければアクセス要求を許可することを特徴とする機密保護方式が得られる。

【０００５】

【実施例】次に本発明について図面を用いて説明する。図１は本発明の一実施例のブロック図、図２はアクセス権定義データ２４２のデータ形式を示す図、図３はファイル属性の形式を示す図、図４は本実施例の動作概要を示すフローチャートである。

【０００６】図１において、ユーザプロセス群１０はユーザプロセス１１および１２からなり、計算機システムに投入される。ファイル群２０はユーザプロセス群１０がアクセスするファイル群で、一般ファイル２１，２２，２３およびアクセス権定義ファイル２４からなる。一般ファイル２１，２２，２３、アクセス権定義ファイル２４はそれぞれファイル属性２１１，２２１，２３１および２４１を持ち、ファイルデータ２１２，２２２，

２３２およびアクセス権定義データ２４２を格納している。

【０００７】ファイル属性２１１，２２１，２３１および２４１は図３の形式となっており、ファイルごとにファイル所有者に対する属性として読出許可，書込許可，実行許可それぞれの可否が設定され、ファイル所有者以外のユーザに対する属性として読出レベル，書込レベル，実行レベルが設定されている。ただし、アクセス権定義ファイル２４に対するアクセスは特権的なアクセスレベルを持つユーザのみがアクセス可能となるよう最高レベルにしている。

【０００８】アクセス権定義データ２４２には、図２に示すように各ユーザの全ての一般ファイル２１，２２，２３に対するアクセス権レベルである読出レベル，書込レベル，実行レベルが予め定義されている。ファイルアクセス部３０はアクセス権判定部３１とファイル入出力部３２とからなる。

【０００９】ファイル入出力部３２は、ユーザプロセス群１０からファイルのアクセス要求があると、ファイル群２０から要求ファイルの属性の情報を取得して、アクセス権判定部３１を呼び出す。アクセス権判定部３１は、属性の情報を読み出し、ユーザがファイルの所有者である場合には、所有者の属性に従ってアクセス判定を行う。一方、ユーザが所有者でない場合には、アクセス権判定部３１はファイル属性で定義しているその他ユーザのアクセス権レベルとアクセス権定義データ２４２中のアクセス権レベルとを比較して、前者のアクセス権レベルが高ければアクセス要求を拒否し、後者のアクセス権レベルの方が高ければアクセス要求を許可する。

【００１０】次に、図４を用いて動作概要を説明する。ユーザプロセス群１０はファイル入出力部３２に対してファイルのアクセス要求を行う（ステップ５１）。ファイル入出力部３２はアクセス権判定部３１を呼び出し、アクセス権判定部３１はファイル群２０から要求ファイルの属性の情報を取得し（ステップ５２）、ユーザがファイル所有者かどうかの判定を行う（ステップ５３）。ユーザがファイル所有者である場合には、アクセス権判定部３１はファイル所有者の属性によりアクセス権の判定を行い（ステップ５４）、アクセス許可時にはファイル入出力部３２に対してファイルへ当該の操作を行うよう指示する（ステップ５７）。

【００１１】一方、アクセス拒否時にはアクセス権判定部３１はエラー処理を行い（ステップ５８）、終了する。また、ユーザがファイル所有者でない場合には、アクセス権判定部３１はファイル入出力部３２を通じてアクセス権定義データ２４２を読み出し（ステップ５５）、ファイルのその他ユーザの属性によりアクセス権の判定を行う（ステップ５６）。判定の結果、アクセス許可時にはアクセス権判定部３１は、ファイル入出力部３２にファイルへ当該の操作を行うよう指示し（ステップ５７）、アクセス拒否時にはエラー処理を行い（ステップ５８）、終了する。

【００１２】

【発明の効果】以上説明したように本発明は、ファイルに対するアクセスの優先度を示すアクセス権レベルをファイル属性として含み、各ユーザプロセスの全ファイルに対するアクセスの優先度を示すアクセス権レベルが予め定義されているアクセス権定義ファイルを持ち、ユーザプロセスがファイルをアクセスするとき、ファイル属性を読み込み、この属性の中のアクセス権レベルとアクセス権定義ファイル中の当該ユーザプロセスの当該ファイルに対するアクセス権レベルとを比較して、ファイルのアクセスの可否をオペレーティングシステム中で判断することにより、各アプリケーションプログラムごとにデータフォーマットを定義する必要がなくなり、データファイルやプログラムの互換性を保つことができる。また、実行形式のファイルに対する機密保護が実現できるという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例のブロック図である。

【図２】図１に示されたアクセス権定義データの形式を示す図である。

【図３】図１に示されたファイル属性の形式を示す図である。

【図４】本実施例の動作概要を示すフローチャート図である。

【符号の説明】

１０　　ユーザプロセス群

１１，１２　　ユーザプロセス

２０　　ファイル群

２１，２２，２３　　一般ファイル

２４　　アクセス権定義ファイル

２１１，２２１，２３１，２４１　　ファイル属性

２１２，２２２，２３２　　ファイルデータ

２４２　　アクセス権定義データ

３０　　ファイルアクセス部

３１　　アクセス権判定部

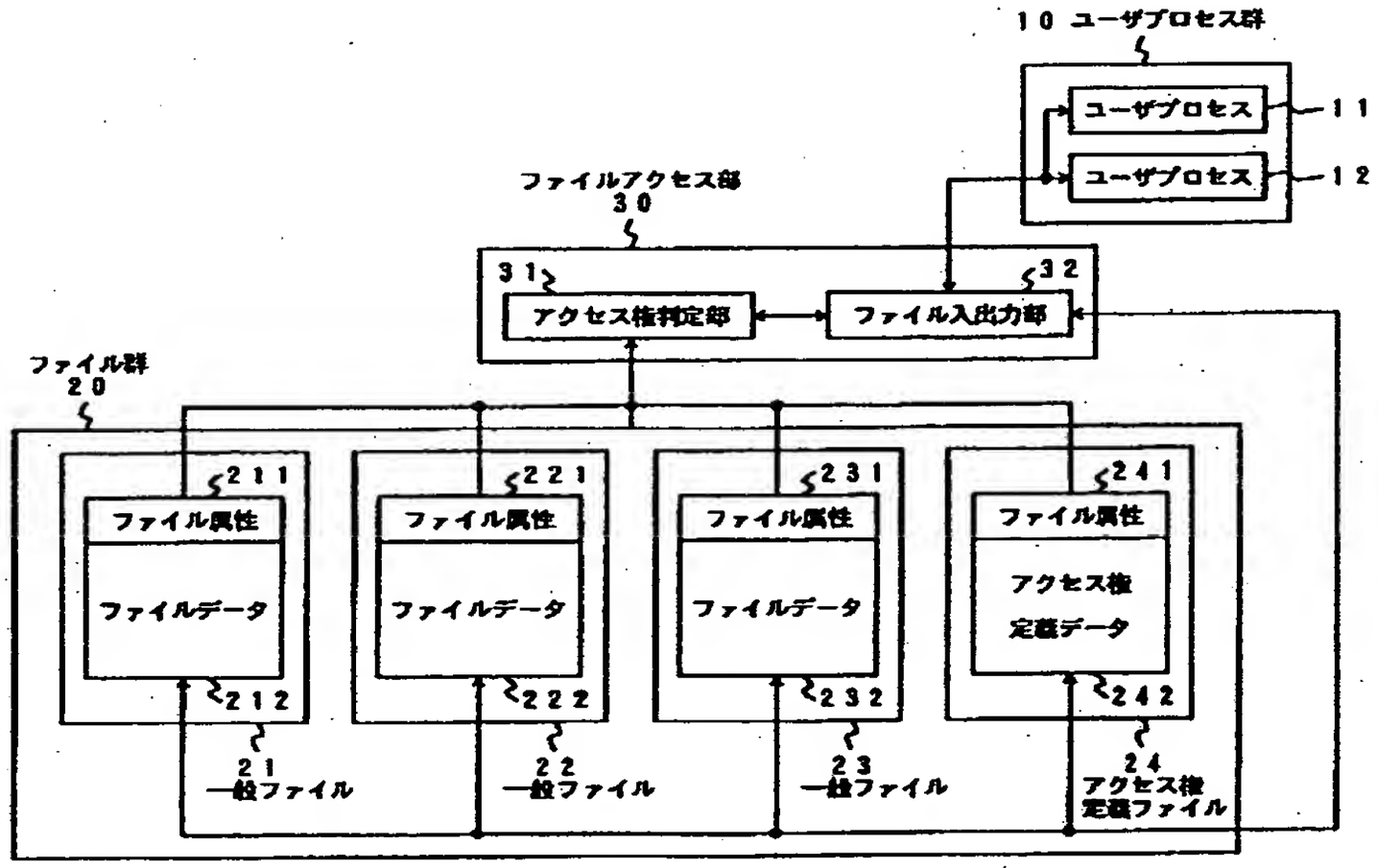
３２　　ファイル入出力部

【図２】

アクセス権定義データ

ユーザＩＤ	読出レベル	書込レベル	実行レベル

【図１】

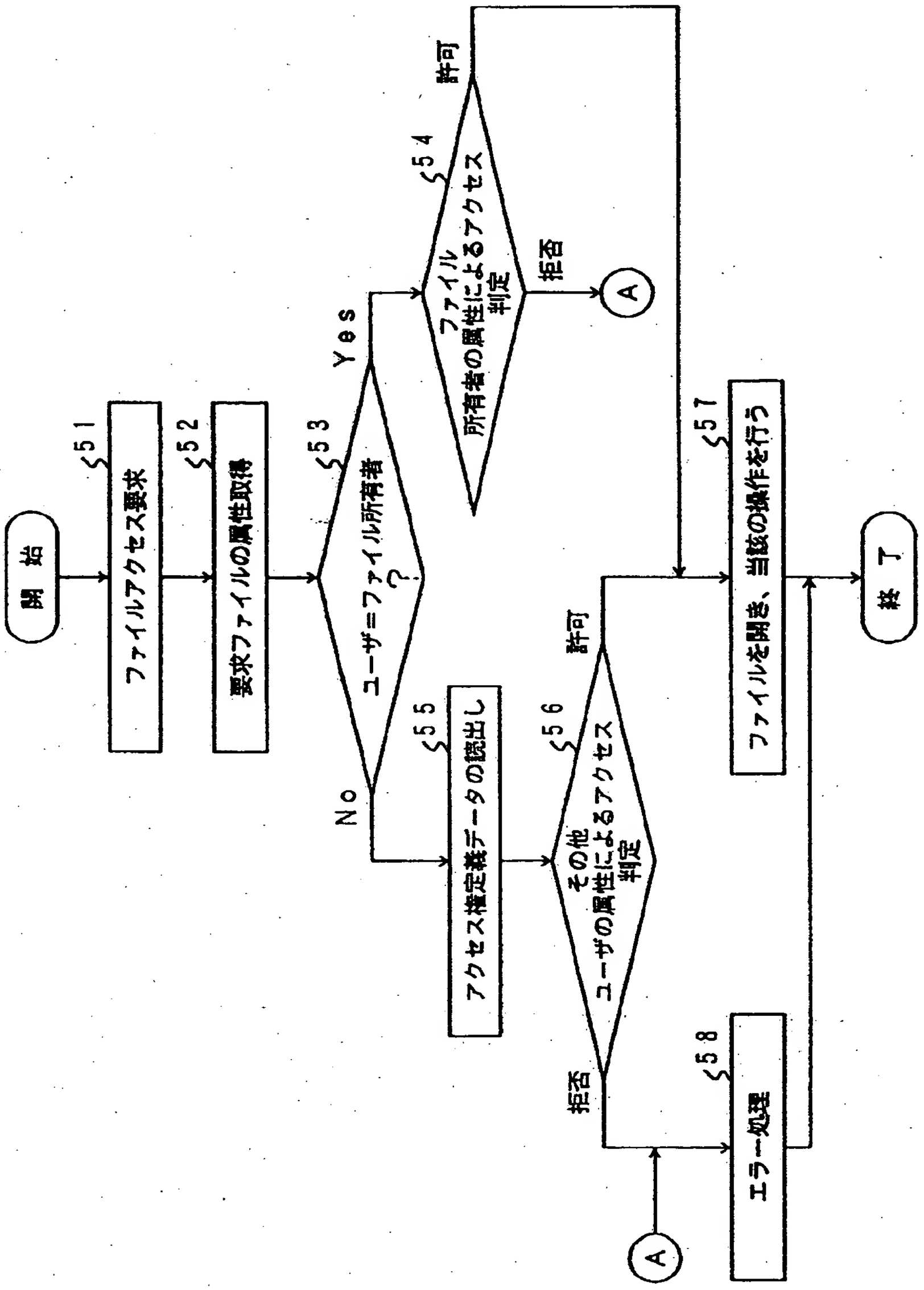


【図３】

ファイル属性形式

ファイル所有者の属性			その他ユーザの特性		
読出許可	書込許可	実行許可	読出レベル	書込レベル	実行レベル

【図４】


開始
S51
ファイルアクセス要求
S52
要求ファイルの属性取得
S53
ユーザ＝ファイル所有者？
Yes
No
S54
ファイルへのアクセスの属性による判定
許可
拒否
S55
アクセス指定データの読出し
S56
その他ユーザの属性によるアクセス判定
許可
拒否
S57
ファイルを開き、当該の操作を行う
S58
エラー処理
終了
A
A